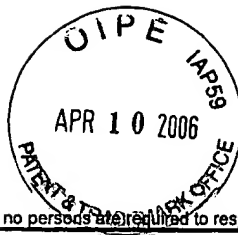


Doc Code: AP.PRE.REQ



Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)

881075-3
681268.0001/1us

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on April 10, 2006

Signature Sarah Schlee

Typed or printed name Sarah Schlee

Application Number

09/770,525

Filed

January 25, 2001

First Named Inventor

Michael Hrabik

Art Unit

2131

Examiner

Jenise E. Jackson

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

* see footnote 1 of Pre-Appeal Brief

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).

Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☒ attorney or agent of record.
Registration number 45,018

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

Anna Vishev
Signature

Anna Vishev
Typed or printed name

(212) 756-2167
Telephone number

April 10, 2006
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



**NOTICE OF APPEAL FROM THE
EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Applicant: Michael Hrabik et al. Examiner: Jenise E. Jackson
Application No.: 09/770,525 Confirmation No.: 5856
Filed: January 25, 2001 Group Art Unit: 2131
For: METHOD AND APPARATUS FOR VERIFYING THE INTEGRITY OF
COMPUTER NETWORKS AND IMPLEMENTATION OF
COUNTERMEASURES

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF

Sir:

Appellant appeals the Examiner's rejection dated January 30, 2006.

1. There is a clear error in the Examiner's Non-Final Rejection¹ of claims 23 and 33 because Emigh does not disclose or suggest a master system which monitors the integrity of a security subsystem as recited in step (b) of claims 23 and 33

The reasons for this clear error are given in Applicants' "Amendment Accompanying RCE" filed December 15, 2005 (mailroom date is December 27, 2005), hereafter, referred to as "the 12/27/05 Response."² See the arguments on pages 8-10 and the accompanying Appendix of the 12/27/05 Response. To summarize, the key argument related to this clear error is that Emigh has no disclosure or suggestion that the NSOC (the alleged "master system") monitors the integrity of the NetRanger sensor (the alleged "security subsystem"). Vulnerability is a completely different concept than integrity, and thus testing for vulnerability is not the same as, or equivalent to, testing for integrity. Vulnerability relates to the susceptibility of a device to attack, whereas integrity

¹ Although the outstanding rejection is a non-final rejection, it is the ninth substantive rejection of the claims on the merits, and thus is ripe for the pre-appeal process.

² The Pre-Appeal guidelines request that prior submissions be referred to by paper number. However, no paper numbers are available to Applicants, nor does any other paper numbering scheme appear on the USPTO's PAIR web site.

relates to whether the device is in a state of being unimpaired. A device can be vulnerable but still have its integrity intact, and vice-versa.

Nor does Messmer make up for this deficiency in Emigh. The Examiner relied upon Messmer only for the “secure link” element of claims 23 and 33.

In paragraph 14 on pages 5-6 of the outstanding rejection, the Examiner responds to the integrity vs. vulnerability argument with the following additional explanations of why Emigh teaches monitoring vulnerability, none of which refute the clear error:

1. The Examiner states that Applicant has not provided in the disclosure a specific definition of the term “integrity.”

In response, there is no requirement to provide a definition for a term that is used in exactly the same manner that the term is known to one of ordinary skill in the art. Likewise, the Examiner is not permitted to give a different meaning to a well-understood term just because no definition is provided in the specification. The Appendix of the 12/27/05 response clearly establishes the ordinary meaning of integrity and vulnerability to one skilled in the computer arts, and demonstrates that these are different concepts.

Furthermore, the specification implicitly defines the meaning of “integrity” and that meaning conforms exactly with the definitions in the Appendix. The “integrity” concept is first introduced on page 3, lines 11-19 of the specification in the following text portion (underlining added for emphasis):

U.S. Pat. No. 5,916,644 to Kurtzberg et al. discloses a method for testing the integrity of security subsystems wherein a specially configured system connected to directly a target computer network will systematically test security on the network by simulating attacks on security devices in order to verify that they are operational. Specifically, the disclosed method randomly simulates an attack on the network. If the attack is detected, the security subsystems are assumed to be functioning. If not, they are considered compromised, and an attack may already be underway. This method is an improvement over passive systems that do not check themselves and therefore cannot properly report on their own status when they have been disabled.

Applicants characterized Kurtzberg as testing to determine if a security subsystem is in a “state of being unimpaired” (i.e., operational or functioning vs. compromised or disabled). Subsequent descriptions of preferred embodiments of the present invention use the word “integrity” in the same manner. See, for example, the following text portions (underlining added for emphasis):

It is another object of the present invention to provide a security system providing integrity verification for security devices on a network, and can also reliably verify its own integrity. (page 4, lines 17-19)

According to another example of the present invention, a pseudo-attack generator associated with the master system is provided that simulates attacks on the target network that should be detected by the subsystem. By comparing the pseudo-attacks made on the target network to the attacks actually detected by the subsystem, the master system can determine whether the integrity of the subsystem has been compromised. (page 5, lines 14-18)

Applicants are not referring to vulnerability testing to determine how susceptible a device is to attack. Applicants are clearly referring to determining whether the security subsystem is in an unimpaired state (e.g., not compromised). The security system may have its integrity intact, but still be highly vulnerable.

In sum, the specification clearly articulates what the scope of the term “integrity” means, the scope conforms with its ordinary meaning to an artisan, and the scope does not encompass “vulnerability.”

2. The Examiner states that Emigh teaches monitoring integrity because if a misuse is found, the alarm will be sent to the master system. The Examiner is presumably referring to the text portion on page 1, lines 33-35 of Emigh.

In response, this text portion appears to refer to misuse of data within a network as a result of a hacker who intrudes into a network. The misuse is thus an indication of “vulnerability,” since it indicates that an unauthorized person was able to obtain access to a network. This is entirely consistent with Emigh because Emigh states that it detects “vulnerability.” Stated simply, if a hacker can gain access to a network, then the network is vulnerable (i.e., susceptible to an attack). Detection of misuse tells us nothing about whether an “integrity” problem exists with respect to the NetRanger sensor, which is the alleged “security subsystem” of Emigh.

3. The Examiner states that since the NSOC monitors the network that uses the NetRanger sensor, and since intrusions can be detected, then Emigh teaches that the NetRanger sensor is in a state of being unimpaired. The Examiner is effectively arguing that as long as intrusions can be detected, the NSOC (i.e., master system) is inherently providing integrity monitoring of the NetRanger sensor (i.e., security subsystem).

In response, the Examiner’s argument is clearly erroneous. The NSOC merely receives whatever reports are sent to it by the NetRanger sensor. The NetRanger may still send reports if it has had its integrity compromised. For example, it may have been compromised in a manner that causes it to send out false reports for certain intrusions, or no reports for certain intrusions, or

reports for intrusions that did not actually occur. The mere fact that the NSOC receives reports from the NetRanger sensor tells us nothing about the integrity of the NetRanger sensor.

In addition to the arguments above, even if it can be somehow justified that testing for vulnerability is the same as testing for integrity (and Applicants strongly disagree that such a justification can be made), Emigh never even states that the NSOC tests the NetRanger sensor for vulnerability. Emigh merely states that network devices like web servers are tested for vulnerability.

In sum, the Examiner has provided no supportable basis for the position that Emigh discloses the “integrity” limitation that is fundamental to meeting step (b) of claims 23 and 33.

2. There is a clear error in the Examiner’s Non-Final Rejection of claim 23 because Emigh does not disclose or suggest a security subsystem that monitors activities of devices on a network as recited in step (a) of claim 23.

The reasons for this clear error are also given in Applicants’ “Amendment Accompanying RCE” filed December 15, 2005 (mailroom date is December 27, 2005), hereafter, referred to as “the 12/27/05 Response.” See the arguments on pages 8-10 of the 12/27/05 Response. To summarize, the key argument related to this clear error is that there is no disclosure or suggestion that Emigh’s NetRanger monitors activities of devices on the corporate network, and that NetRanger merely detects and analyzes IP network traffic (i.e., traffic among and between devices on the network). Stated simply, monitoring activities of devices on a network is a different function than detecting and analyzing IP network traffic. Each can be performed independent of the other. Just because one of these functions is being performed, it doesn’t necessarily mean that the other is being performed.

In paragraph 15 on page 6 of the outstanding rejection, the Examiner provides the following additional explanations of why Emigh teaches this limitation, none of which refute the clear error:

1. The Examiner states that NetRanger monitors devices on the network because NetRanger is located on places within the corporate network such as Internet and Intranet connections. These connections monitor traffic which represents activities of these devices, such as intrusions or misuse.

In response, the Examiner is reading unstated functionality into Emigh. Emigh clearly states that signatures indicative of misuse are “defined by the customer.” (page 1, line 34). Nowhere does Emigh describe that a particular signature indicates an activity of an actual device on the corporate network. A signature indicative of misuse may have nothing whatsoever to do with the activity of

an actual device on the corporate network. More generally, traffic on the network may have nothing whatsoever to do with the activity of an actual device on the corporate network.

Consider a simple example of a data message that consists of a request to access a secure location of a web server. If that data message is detected at a particular location in a corporate network where it is not expected to exist (e.g., a public gateway to the corporate network, instead of a secured intranet gateway to the corporate network), then it may be considered to be a hacker attempt, and NetRanger could be programmed to detect such an occurrence. However, this does not mean that any particular activity occurred on a network device, such as the web server which may be programmed to reject all requests from non-intranet sources.

In sum, it is clear error to presume that NetRanger has capabilities that are not described in the applied reference.

2. The Examiner states that claim 23 does not distinguish between what types of attacks may occur with respect to network devices.

The Examiner raises this point in response to Applicants' discussion on page 9, second full paragraph, of the 12/27/05 Response which explains that devices can be attacked even if there is no suspicious IP network traffic, and thus merely monitoring IP traffic is not sufficient to detect all attacks on network devices. In this paragraph, Applicants were merely highlighting one benefit of the present invention over a hypothetical scheme that relies only on "IP network traffic" to detect attacks on network devices. However, since this issue does not focus directly on the claim limitation at issue, namely, the monitoring of activities of devices on a network, this discussion can be ignored in deciding whether there is clear error in the outstanding rejection for the reasons stated above.

3. There is a clear error in the Examiner's Non-Final Rejection of the dependent claims.

The rejected dependent claims are believed to be allowable because they depend upon respective allowable independent claims, and because they recite additional patentable steps.

4. None of the arguments above depend upon interpretations of prior art teachings or claim scope issues. For at least the reasons set forth above, all of the outstanding rejections should be withdrawn.

Respectfully submitted,

SCHULTE ROTH & ZABEL LLP
Attorneys for Appellants
919 Third Avenue
New York, New York 10022

By: Anna Vishev
Anna Vishev
Reg. No. 45,018

Dated: April 10, 2006
New York, New York

CERTIFICATE OF EXPRESS MAILING

Date of Deposit:
April 10, 2006

Express Mail Label No.:
EV325882295US

I hereby certify under 37 C.F.R. 1.10 that this correspondence and enumerated documents are being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" with sufficient postage on the date indicated above and is addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Name:

Sarah Schlie

Signature:

Sarah Schlie
Schulte Roth & Zabel, LLP
